Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] A method of secure data exchange between a master cryptographic unit and a slave cryptographic unit, comprising the steps of:
sending either a reset message or a key validation message to request the master cryptographic unit to validate a key held by the slave cryptographic unit; and
forwarding a key exchange message, which includes a new key encrypted through the key held by the slave cryptographic unit, from the master cryptographic unit to the slave cryptographic unit.

[c2] The method of secure data exchange of Claim 1, further comprising a step of sending a key confirmation message to notify the master cryptographic unit that the new key is correctly received by the slave cryptographic unit.

[c3] The method of secure data exchange of Claim 2, further comprising the steps of:
responding to the key confirmation message with a downloading message to allow the slave cryptographic unit retrieving requested information; and
sending a finish message to the master cryptographic unit after the requested information is completely down-

loaded.

[c4] The method of secure data exchange of Claim 1, wherein the reset message requests the master cryptographic unit to validate an initial key held by the slave cryptographic unit.

[c5] The method of secure data exchange of Claim 4, wherein the initial key is either pre-configured by factories and permanently stored in the slave cryptographic unit or obtained from the master cryptographic unit through a manual login.

[c6] The method of secure data exchange of Claim 1, further comprising a step of notifying the slave cryptographic unit that the key is invalid after the key validation message is sent.

[c7] The method of secure data exchange of Claim 6, further comprising a step of sending the rest message to request the master cryptographic unit to validate an initial held by the slave cryptographic unit.

[c8] The method of secure data exchange of Claim 3, further comprising the steps of:
sending another key validation message to request the master cryptographic unit to validate the new key held by the slave cryptographic unit; and

forwarding another key exchange message, which includes a renewed key encrypted through the new key held by the slave cryptographic unit.

[c9] The method of secure data exchange of Claim 1, further comprising a step of notifying the slave cryptographic unit that the key is invalid after the resent message is sent.

[c10] The method of secure data exchange of Claim 1, wherein the master cryptographic unit is a key distribution server.

[c11] The method of secure data exchange of Claim 10, wherein the key distribution server is included in an automatic provisioning system.

[c12] The method of secure data exchange of Claim 10, wherein the slave cryptographic unit is a client.

[c13] The method of secure data exchange of Claim 10, wherein the reset message includes an initial key, a physical address of the slave cryptographic unit, timestamp data and hash data.

[c14] The method of secure data exchange of Claim 10, wherein the key validation message includes the key, a physical address of the slave cryptographic unit, times-

tamp data and hash data.